Gillian L. Wade, State Bar No. 229124
gwade@milsteinadelman.com
Sara D. Avila, State Bar No. 263213
savila@milsteinadelman.com
**MILSTEIN ADELMAN LLP**
2800 Donald Douglas Loop North
Santa Monica, California 90405
Telephone: (310) 396-9600
Fax: (310) 396-9635

Bryan L. Clobes (to apply *pro hac vice*)
bclobes@caffertyclobes.com
Kelly Tucker (to apply *pro hac vice*)
ktucker@caffertyclobes.com
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**
1101 Market Street
Philadelphia, PA 19107
Phone: (215) 864-2800
Facsimile: (215) 864-2810

Daniel O. Herrera (to apply *pro hac vice*)
dherrera@caffertyclobes.com
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**
30 North LaSalle Street
Suite 3200
Chicago, Illinois 60602
Telephone: (312) 782-4880
Facsimile: (312) 782-7785

Attorneys for Plaintiff,
Jennifer Leitner and the Proposed Class

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

JENNIFER LEITNER, on behalf of herself, and others similarly situated,

Plaintiffs,

vs.

EXPERIAN INFORMATION SOLUTIONS, INC.; and DOES 1 through 100, inclusive,

Defendants.

CASE NO.: 8:15-cv-01620-JLS-KES

**FIRST AMENDED CLASS ACTION COMPLAINT**

1. WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA") 15 U.S.C. § 1681, et seq.)
2. NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT (15 U.S.C. § 1681, *et seq.*)
3. VIOLATION OF THE CALIFORNIA DATA BREACH ACT (Cal. Civ. Code §§ 1798.80, *et seq.*)
4. VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT (815 ILCS 505/1, *et seq.*)
5. BREACH OF IMPLIED CONTRACT
6. NEGLIGENCE
7. BAILMENT
8. VIOLATION OF BUSINESS & PROFESSIONS CODE § 17200, *et seq.*

**DEMAND FOR JURY TRIAL**

Plaintiff Jennifer Leitner, on behalf of herself and all persons similarly situated, by and through her attorneys, alleges personal knowledge as to all facts related to herself and on information and belief as to all other matters, which are based upon, among other things, the investigation made by Plaintiff through her counsel:

**PRELIMINARY STATEMENT**

1. Plaintiff Jennifer Leitner ("Plaintiff") brings this action on behalf of herself and all other similarly situated individuals who applied for T-Mobile US, Inc. ("T-Mobile") postpaid services or device financing between September 1, 2013, and September 16, 2015 (the "Class").

2. T-Mobile is one of the nation's two largest mobile cellular and data providers in the United States, with over 56.8 million subscribers as of March 31, 2015. As part and parcel of its business operations, T-Mobile subjects applicants for postpaid (as opposed to prepaid) services to routine credit checks in order to determine the services for which they qualify, and Experian Information Solutions, Inc. ("Experian" OR "Defendant") conducts these credit checks pursuant to its contractual relationship with T-Mobile. Class members trusted Experian and provided their highly valuable personal data with the belief that IT would act with reasonable care and protect it from disclosure. Unfortunately, Experian retained Class members' data on inadequately secured servers accessible to those with the means and malice to place the identities of millions at risk.

3. On October 1, 2015, Experian revealed that it had suffered a catastrophic data breach of its information technology ("IT") system (the "Breach"). The hackers gained access to servers containing sensitive and confidential data entrusted to Defendant by approximately 15 million persons who applied for T-Mobile services, including persons who never purchased products or services from T-Mobile. The compromised data includes full names, Social Security numbers, alternative identification (e.g., driver's license) numbers, addresses, phone numbers, email addresses, employment information (including income data), dates of birth, and other

personal information ("Personal Data").

4. Defendant experienced this catastrophic data breach they failed to develop, maintain, and implement sufficient security measures on the relevant databases. Indeed, this Breach follows in the wake of a number of widely publicized data breaches affecting companies such as Anthem, Target, Home Depot, Neiman Marcus, Community Health Systems, Inc., Michaels Stores, Jimmy Johns, Sony Entertainment, J.P. Morgan Chase & Co., P.F. Changs, Staples, and others. But notwithstanding these earlier data security incidents, Defendant failed to take adequate steps to prevent the Breach from occurring.

5. Not only did Defendant fail to take appropriate measures to prevent the Breach from occurring in the first instance, its subsequent remedial efforts are wholly insufficient to protect those individuals whose personal information has now been compromised. Defendant is offering credit monitoring protection for a period of only two years despite expert consensus that identity theft victims are at risk of significant harm for five to ten years following a breach. Moreover, in light of the perpetrators' immediate efforts to monetize this information, as well as the sensitive nature of the Personal Data, Defendant's offered relief is woefully inadequate.

6. Plaintiff, individually and on behalf of the Class defined below, seeks to hold Defendant accountable for the Breach by ensuring that it provides adequate protection to those affected. Plaintiff seeks relief for Defendant's violations of certain statutes discussed *infra*, breach of contractual obligations, negligence, violations of certain statutes discussed *infra*, bailment and, alternatively, unjust enrichment.

## JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one plaintiff and defendant are citizens of different states.

8. This Court has federal question jurisdiction under 28 U.S.C. § 1331 in light of the Fair Credit Reporting Act alleged below.

9. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this judicial district and division pursuant to 28 U.S.C. § 1391. A substantial part of the events and/or omissions giving rise to the claims occurred within this district and division. Additionally, Defendant resides here as it maintains its principle office and headquarters in this District.

## PARTIES

11. Plaintiff Jennifer Leitner is a resident of the state of Illinois. Her personal information was compromised as part of the Breach announced by Defendant on October 1, 2015. Plaintiff has already spent time addressing this data breach by investigating whether she was affected and investigating measures to protect herself from identity theft. Plaintiff contacted T-Mobile, which confirmed that she applied for postpaid services during the period in question, but neither Defendant nor T-Mobile have notified her that she was impacted by the Breach. As a result of Defendant's conduct, Plaintiff has been injured.

12. Defendant Experian Information Solutions, Inc., is an entity incorporated in the State of Delaware with its headquarters and principal place of business located at 475 Anton Blvd. Costa Mesa, California 92626.

## FACTUAL ALLEGATIONS

13. T-Mobile subjects all prospective customers who wish to purchase postpaid services or finance device purchases to credit checks conducted by Experian. The number of credit checks performed by Experian on behalf of T-Mobile has jumped over the past two years as the third-largest wireless network in the United States has grown at a blistering pace, adding roughly one million new customers each quarter and far outpacing its larger rivals.

14. Experian is obligated by law to retain the personal information T-Mobile

requires Plaintiff and Class members to submit in connection with these applications for a period of 25 months. Experian failed to safeguard this information, however, and Plaintiff and the Class's Personal Data has now fallen into the wrong hands.

15. On or about October 1, 2015, Experian notified T-Mobile and the public that Experian experienced "an unauthorized acquisition of information" from a server containing T-Mobile-related data, including the Personal Data of approximately 15 million persons who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015. According to Experian, "[t]he data acquired included names, dates of birth, addresses, and Social Security numbers and/or an alternative form of ID like a drivers' license number, as well as additional information used in T-Mobile's own credit assessment."[1]

16. This is not the first breach sustained by Experian. An attack on an Experian subsidiary that began before Experian purchased it in 2012 exposed the Social Security numbers of 200 million Americans and prompted an investigation by at least four states.

**Plaintiff and the Class have Suffered Harm**

17. Like any data hack, the instant Breach presents major problems for all affected. Said Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[2]

18. The FTC warns the public to pay particular attention to how they keep personally identifying information: Social Security numbers, financial information, and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft." And once they have this information, "they can drain

[1] http://www.prnewswire.com/news-releases/experian-notifies-consumers-in-the-us-who-may-have-been-affected-by-unauthorized-acquisition-of-a-clients-data-300152926.html (last visited Oct. 6, 2015).
[2] http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/ (last visited Oct. 6, 2015).

your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

19. The ramifications of Defendant's failure to properly secure Plaintiff's and the Class' Personal Data are severe. Identity theft occurs when someone uses another person's medical, financial, and personal information, such as that person's name, address, Social Security Number, medical and insurance information, financial account information, and other information, without permission to commit fraud or other crimes.

20. According to data security experts, one out of four data breach notification recipients became a victim of identity fraud.

21. Identity thieves can use the Personal Data of Plaintiff and the Class, which Defendant failed to keep secure, to perpetuate a variety of crimes that harm the victims including immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, filing a fraudulent tax return using the victim's information to obtain a fraudulent refund, fraudulently obtaining a loan tied to the victim's credit and personal information, and fraudulently opening other accounts in the name of the victim.

22. Moreover, the data compromised in the Breach has no expiration date. While credit card numbers and the like may become useless after some time, personal identification numbers and Social Security numbers do not. The United States government and privacy experts acknowledge that when such data is compromised, it may take years for identity theft to come to light.

23. Indeed, Plaintiff's and the Class' Personal Data has already made its way to the darkest and most nefarious corners of the web. On October 3, 2015, Trustev, an Irish fraud prevention company which monitors such data sales listings, released

screen shots of listings for Personal Data compromised during the breach.[3]

24. Commentators believe these developments may "spell financial doom" for millions.[4] "This is a bad one," agreed Rurik Bradbury, chief marketing officer at Trustev, an e-commerce security company. "That's the problem for the 15 million. The amount of data is enough to do a lot of damage. Complete identities have been stolen."

**Defendant's Security Protocols and Response to the Breach Are Inadequate**

25. The safeguards employed by Defendant prior to the breach appear to have been lacking. The speed with which the Class' Personal Data found its way to the dark web suggests that Experian may not have encrypted the Personal Data stored on its servers, or that its encryption efforts were lacking.[5]

26. Defendant's subsequent response also has been woefully deficient. Defendant has offered Plaintiff and Class members only two years of credit monitoring despite the fact they will face an increased risk of identity theft due to a breach for the rest of their lives. Unlike credit card and bank account numbers, the compromised Personal Data does not expire. Plaintiff cannot change her Social Security number or her driver's license number as a preventative measure, and she is now subject to the misappropriation of her Personal Data for years to come.

27. That the credit monitoring offered by Defendant will be carried out by Experian itself raises further concerns. Defendant is effectively asking affected persons to choose to trust in the very entity that placed them in this predicament: Experian. That choice is no choice at all.

28. As a direct and proximate result of Defendant's actions and omissions in disclosing and failing to protect Plaintiff's private personal information, Plaintiff and those similarly situated have been placed at a substantial risk of harm in the form of

[3] http://venturebeat.com/2015/10/03/data-likely-stolen-from-experiant-mobile-spotted-for-sale-on-dark-web-says-security-firm/ (last visited Oct. 6, 2015).

[4] http://www.thestreet.com/story/13312302/2/why-the-experian-t-mobile-hack-may-bring-financial-doom-to-millions.html (last visited Oct. 6, 2015).

[5] *Id.*

identity theft and have incurred and will incur actual damages in an attempt to prevent identity theft.

## CLASS ALLEGATIONS

29. Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a class of

> All United States residents who applied for T-Mobile US, Inc. postpaid services or device financing between September 1, 2013, and September 16, 2015 (the "Class").
>
> Excluded from the Class is Defendant, its executives, officers, and the Judge(s) assigned to this case.

Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

30. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of

> All Illinois residents who applied for T-Mobile US, Inc. postpaid services or device financing between September 1, 2013, and September 16, 2015 (the "Illinois Class").
>
> Excluded from the Illinois Class is Defendant, its executives, officers, and the Judge(s) assigned to this case.

31. Numerosity: The Class is so numerous that joinder of all members is impracticable. Defendant has acknowledged that approximately 15 million records may have been compromised by the Breach.

32. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to:

a. whether Defendant's data security and retention policies were unreasonable;

b. whether Defendant failed to protect the confidential and highly

sensitive information with which they were entrusted;

c. whether Defendant breached any legal duties in connection with the data breach;

d. Whether Defendant's conduct was intentional, reckless, willful or negligent;

e. Whether Defendant violated the Federal Credit Reporting Act;

f. whether Defendant was negligent;

g. whether Defendant was unjustly enriched;

h. whether Plaintiff and Defendant entered into a bailment arrangement, which was breached; and

i. whether Plaintiff and Class Members are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

33. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their Personal Data compromised in the Breach.

34. Adequacy: Plaintiff is an adequate representative because her interests do not materially or irreconcilably conflict with the interests of the Class that she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and she intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

35. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court

system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases. Indeed, Defendant claims to already be in the process of notifying them.

36. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

## CAUSES OF ACTION
## COUNT I
## WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

37. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

38. Pursuant to 15 U.S.C. § 1681a(f), a "consumer reporting agency" includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing "consumer reports" to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

39. Pursuant to 15 U.S.C. § 1681a(d)(1), a "consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in

establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

40. "Consumer credit information" includes, *inter alia*, a person's name, identification number (e.g., Social Security number), marital status, physical address and contact information, educational background, employment, professional or business history, financial accounts and financial account history (i.e. details of the management of the accounts), credit report inquiries (i.e. whenever consumer credit information is requested from a credit reporting agency), judgments, administration orders, defaults, and other notices.

41. FCRA limits the dissemination of "consumer credit information" to certain well-defined circumstances and no other. 15 U.S.C. § 1681b(a).

42. At all relevant times, Experian was (and continues to be) a consumer reporting agency under FCRA because on a cooperative nonprofit basis and for monetary fees, it regularly (i) received, assembled and/or evaluated Plaintiff's and Class members' "consumer credit information" protected by FCRA for the purpose of furnishing consumer reports to third parties, and (ii) used the means and facilities of interstate commerce to prepare, furnish and transmit consumer reports containing Plaintiff's and Class members' consumer credit information to third parties (and continues to do so).

43. As a consumer reporting agency, Defendant was (and continues to be) required to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard, protect and limit the dissemination of consumer credit information in its possession, custody and control, including Plaintiff's and Class members' consumer credit information, only for permissible purposes under FCRA. *See* 15 U.S.C. § 1681(b).

44. By its above-described wrongful actions, inaction and omissions, want of

ordinary care, and the resulting security breach, Defendant willfully and recklessly violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' consumer credit information.

45. Defendant's above-described wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and proximately caused the security breach which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiff's and Class members' consumer credit information into the public domain for no permissible purpose under FCRA. Defendant's above described willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiff and Class members about the security breach which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiff and Class members.

46. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting security breach, directly and proximately caused Plaintiff and Class members to suffer economic damages and other actual injury and harm, and collectively constitute the willful and reckless violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class members' consumer credit information would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit identity fraud. Plaintiff and Class members, therefore, are entitled to declaratory relief, injunctive relief, and compensation for their economic damages, and other actual injury and harm in the form of, *inter alia*, (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their consumer credit information, for which there is a well-established national and international market, (iii) the financial and temporal cost of monitoring their credit,

monitoring their financial accounts, and mitigating their damages, and (iv) statutory damages of not less than $100, and not more than $1,000, each, under 15 U.S.C. § 1681n(a)(1).

47. Plaintiff and Class members also are entitled to recover punitive damages, under 15 U.S.C. § 1681n(a)(2), and their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681n(a)(3).

**COUNT II**
**NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**
**(15 U.S.C. § 1681, *et seq.*)**

48. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

49. In the alternative, by its above-described wrongful actions, inaction and omissions, want of ordinary care, and the resulting security breach Defendant negligently or in a grossly negligent manner violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a); (g), and 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' consumer credit information.

50. Defendant's above-described wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and/or proximately caused the security breach which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiff's and Class members' consumer credit information into the public domain for no permissible purpose under FCRA. Defendant's above-described willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiff and Class members about the security breach which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiff

and Class members.

51. It was reasonably foreseeable to Defendant that its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' consumer credit information would result in a security lapse, whereby unauthorized third parties would gain access to, and disseminate, Plaintiff's and Class members' consumer credit information into the public domain for no permissible purpose under FCRA.

52. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting security breach, directly and proximately caused Plaintiff and Class members to suffer economic damages and other actual injury and harm, and collectively constitute the negligent violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class members' consumer credit information would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit identity fraud. Plaintiff and Class members, therefore, are entitled to declaratory relief, injunctive relief, and compensation for their economic damages, and other actual injury and harm in the form of, *inter alia*, (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their consumer credit information, for which there is a well- established national and international market, and (iii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

54. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681o(a)(2).

## COUNT III
## VIOLATION OF THE CALIFORNIA DATA BREACH ACT
## (Cal. Civ. Code §§ 1798.80, *et seq.*)

55. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

56. Plaintiff is a "consumer" within the meaning of California's Data Breach Act, Cal. Civ. Code § 1798.80(c).

57. Defendant is a "business" within the meaning of Cal. Civ. Code § 1798.80(a).

58. Pursuant to Cal. Civ. Code §§ 1798.80(e), 1798.81.5(d)(1) and 1798.82(h), the sensitive and unencrypted customer information misappropriated from Defendant includes Plaintiff's and other Class members' "personal information," including names, Social Security numbers, street addresses , and driver's license or state identification card numbers.

59. Defendant "owns" or "licenses" this personal information within the meaning of Cal. Civ. Code § 1798.81.5(a)(2) because Defendant retains this information as part of its internal customer accounts or for the purpose of using that information in transactions with the persons to whom the information relates.

60. By failing to take reasonable steps to protect and safeguard Plaintiff's and the Class' unencrypted Personal Data from unauthorized access, use or disclosure as set forth above, Cal. Civ. Code § 1798.81.5(b), Defendant violated the California Data Breach Act. Defendant's protections are and were unreasonable. Upon information and belief, Defendant not only failed to encrypt Plaintiff's and the Class' Personal Data, but also failed to safeguard it as they did sensitive and critical personal information of other persons located on other servers.

61. Defendant also unreasonably delayed informing Plaintiff and members of the Class about the security breach of Class Members' confidential and non-public information immediately following discovery of the same. The public notice provided generally to Plaintiff and the Class thus far also fails to comply with the specific notice requirements set forth in the Act. *See* Cal. Civ. Code § 1798.82(b).

62. Defendant's violations of the Act proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

63. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses, costs, and civil penalties under Cal. Civ. Code §§ 1798.84 (c) and (g).

**COUNT IV**
**VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT**
**(815 ILCS 505/1, *et seq.*)**
**(On Behalf of the Illinois Class)**

64. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

65. This count is brought against Defendant pursuant to the Illinois Consumer Fraud and Deceptive Trade Practices Act, 815, ILCS 505/1, *et seq.* ("ICFA").

66. At all times relevant herein, the ICFA was in effect. The ICFA prohibits "unfair and deceptive practices."

67. Plaintiff and members of the Class are consumers.

68. A violation of the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/1, *et seq.*, "constitutes an unlawful practice under the [ICFA]." IPIPA § 20.

69. Defendant is a "Data Collector[]" within the meaning of IPIPA § 5.

70. The Breach experienced by Defendant constitutes a "breach of the security of the system data" within the meaning of IPIPA § 5.

71. Pursuant to the IPIPA, the sensitive and unencrypted customer information misappropriated from Defendant includes Plaintiff's and other Class members' "personal information," including names, Social Security numbers, and

driver's license or state identification card numbers. IPIPA § 5.

72. Defendant has unreasonably delayed informing Plaintiff and members of the Class about the security breach of Class Members' confidential and non-public information immediately following discovery of the same. The public notice provided generally to Plaintiff and the Class thus far also fails to comply with the specific notice requirements set forth in the Act. *See* IPIPA § 10(a)-(b). Defendant has therefore violated the IPIPA and engaged in unlawful practices in violation of the ICFA.

73. Defendant's violations of the ICFA proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

74. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under the ICFA.

**COUNT V**
**BREACH OF IMPLIED CONTRACT**
**(Against Experian on Behalf of the Class or, in the Alternative, the Illinois Class)**

75. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

76. Under the facts and circumstances of this case, there was an implied contractual agreement pursuant to which, in exchange for Plaintiff and Class Members providing their Personal Data to Defendant (for its benefit), Defendant would take reasonable and appropriate measures to safeguard and prevent it from being disclosed to unauthorized third parties.

77. Defendant's breach of these obligations proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

## COUNT VI
## NEGLIGENCE
## (On Behalf of the Class or, in the Alternative, the Illinois Class)

78. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

79. Defendant had a duty to, *inter alia*, take reasonable measures to protect the Personal Data entrusted to them.

80. Defendant breached this duty by knowingly and intentionally failing to adequately safeguard the Personal Data of Plaintiff and the Class, or to take commercially reasonable measures to protect that Personal Data.

81. Defendant was legally obligated to timely disclose the Breach to Plaintiff and Class members.

82. Defendant failed to timely notify Plaintiff and the Class, thereby preventing Class Members from taking meaningful, proactive steps to investigate possible identity theft.

83. In light of the recent data breaches in the news, it was reasonably foreseeable that its failure to safeguard this data would injure Plaintiff and Class Members.

84. Defendant's breach proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

## COUNT VII
## BAILMENT
## (On Behalf of the Class or, in the Alternative, the Illinois Class)

85. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint. This count is plead in the alternative to the contract-based claims.

86. Plaintiff and Class members delivered and entrusted their Personal Data to Defendant for the sole purpose of receiving services from them.

87. During the time of bailment, Defendant owed Plaintiff and Class members a duty to safeguard this information properly, and to maintain reasonable security procedures and practices to protect such information. Defendant breached this duty.

88. Defendant's breach proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

## COUNT VIII
## VIOLATIONS OF THE CALIFORNIA BUSINESS & PROFESSIONS CODE §§ 17200, *ET SEQ.*
## (On Behalf of the Class or, in the Alternative, the Illinois Class)

89. Plaintiff incorporates by this reference the allegations contained in the preceding paragraphs as if fully set forth herein.

90. This cause of action is brought pursuant to Business & Professions Code §§17200, *et seq.* on behalf of Plaintiff and the Class.

91. As alleged herein and above, Plaintiff has standing to pursue this claim because she has suffered injury in fact and has lost money or property as a result of Defendant's actions set forth herein. Specifically, prior to filing this action, Plaintiff provided her Personal Data to Defendant. In doing so, Plaintiff trusted Defendant with their highly valuable personal data with the belief that Defendant would act with reasonable care and protect it from disclosure, as referenced above. Plaintiff was affected by the Breach and spent time investigating measures to protect herself from

identity theft. Plaintiff would not have provided her personal data for a credit check had Plaintiff known Experian, with T-Mobile's full knowledge, would retain her data on inadequately secured servers accessible to those with the means and malice to place her, and the identities of millions of others, at risk.

92. Defendant's business practices, as alleged herein, are unfair because: (1) the injury to the consumer is substantial; (2) the injury is not outweighed by any countervailing benefits to consumers or competition; and (3) consumers, including Plaintiff and the Class, could not have avoided the injury because in order to determine the T-Mobile services for which consumers qualify, they were required to undergo a credit check through Experian.

93. Defendant represented to Plaintiff and the Class that their Personal Data would be adequately safeguarded. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive customers into believing Defendant will adequately safeguard customers' Personal Data.

94. Defendant's business practices as alleged herein also constitute illegal and unlawful business practices committed in violation of Business & Professions Code § 17200 because Defendant has also violated 15 U.S.C. §§ 1681, *et seq.*, Cal. Civ. C. §§ 1798.80, *et seq.*, 815 ILCS §§ 505/1, *et seq.* and the common law.

95. Defendant's unfair business practices constituted, and constitute, a continuing course of conduct of unfair competition since Defendant is collecting and storing consumers' information without adequate safeguards to protect the information.

96. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the conduct described herein.

97. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from engaging in the unfair competition alleged herein in connection with the collection and maintenance of Plaintiff and the Class' Personal Data. Additionally, Plaintiff requests an order

awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of the unfair competition alleged herein.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and members of the Class, respectfully requests that this Court:

A. Determine that the claims alleged herein may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and issue an order certifying the Class as defined above;

B. Appoint Plaintiff as the representative of the Class and her counsel as Class counsel;

C. Award all actual, general, special, incidental, statutory, and consequential damages to which Plaintiff and Class Members are entitled;

D. Award pre-judgment and post-judgment interest on such monetary relief;

E. Grant appropriate injunctive and/or declaratory relief;

F. Award reasonable attorneys' fees and costs; and

G. Grant such further relief that this Court deems appropriate.

Dated: October 16, 2015

**MILSTEIN ADELMAN, LLP**

By: *s/ Gillian L. Wade*
Gillian L. Wade
Sara D. Avila

Bryan L. Clobes
Kelly Tucker
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**

Daniel O. Herrera
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**

Attorneys for Plaintiff,
Jennifer Leitner and the Proposed Class

**DEMAND FOR JURY TRIAL**

Plaintiff respectfully demands a trial by jury on all issues so triable.

Dated: October 16, 2015

**MILSTEIN ADELMAN, LLP**

By: *s/ Gillian L. Wade*
Gillian L. Wade
Sara D. Avila

Bryan L. Clobes
Kelly Tucker
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**

Daniel O. Herrera
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**

Attorneys for Plaintiff,
Jennifer Leitner and the Proposed Class

**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on this 16th day of October, 2015, I electronically filed the forgoing with the Clerk of Court using the CM/ECF system which will send notification of filing to all counsel of record listed below:

Richard J. Grabowski
**Jones Day**
3161 Michelson Drive, Suite 800
Irvine, CA 92612-4408
Telephone: (949) 851-3939
Fax: (949) 553-7539
Email: rgrabowski@jonesday.com

I HEREBY FURTHER CERTIFY that a true and correct copy of this filing was also mailed to the party listed below via US Mail:

Corporation Service Company
Registered Agent for
T-Mobile US, Inc.
2711 Centerville Rd.
Wilmington, DE 19808

By: s/ *Gillian L. Wade*
Gillian L. Wade